Available online at www.sciencedirect.com

ScienceDirect

Procedia - Social and Behavioral Sciences 129 (2014) 453 – 459

Procedia Social and Behavioral Sciences

ICIMTR 2013

International Conference on Innovation, Management and Technology Research, Malaysia, 22 – 23 September, 2013

Intrusion Detection Systems in MANET: A Review

Ehsan Amiri[a*], Hassan Keshavarz[b], Hossein Heidari[c], Esmaeil Mohamadi[d], Hossein Moradzadeh[e]

[a,c,e]*Nourabad Mamasani Branch, Islamic Azad University, Nourabad Mamasani, Iran*

[b]*Management of Technology Department, MJIIT, Universiti Teknologi Malaysia, Jalan Semarak,54100 Kuala Lumpur, Malaysia*

[d]*Department of Computer Engineering,Shiraz University, Iran*

[e]*School of Engineering and Technology, Asia Pacific University of Technology and Innovation, Malaysia*

Abstract

Mobile Ad hoc Network consists of some nodes that are stand randomly in operational environment. Because nodes are without any predefined infrastructure and mobility then that are susceptible for intrusion and attack. Securing is an important field in this type of network. In this paper we aim to representing concept of intrusion detection and then survey some of major intrusion detection approach in MANET and aim to comparing in some important field such as: use methods, type of attacks addressed, overhead, and architecture.

Keywords: Intrusion detection; MANET; attacks.

1. Introduction

MANETs consist of some wireless mobile nodes with limitations such as remaining energy, network life time, security and etc. Maybe we could say security is the important limitation. MANET due to nodes mobility and dynamic topology that is frequently change is very susceptible to a variety of attacks such as eavesdropping, routing, packet modification, etc. and securing a MANET under such conditions is

* Corresponding author. Tel.: +98-917-989-1610.
E-mail address: amireehsan@gmail.com.

doi:10.1016/j.sbspro.2014.03.700

challenging. An effective way to identify when an attack occurs in a MANET is the deployment of an Intrusion Detection System (IDS) (Panos, Xenakis & Stavrakakis, 2010).

The IDS system is an integrated method for detect any attacks by analyzing and continues monitoring network activities. Intrusion detection systems can be run on each mobile node to check local traffic and detect local intrusions. These nodes can communicate local intrusion information to each other as and when needed. Figure1 show the local model of intrusion detection system. Each node has local IDS that by this, node can connect to network and local IDS checking all send or receive data in/out node. Other technique is to run intrusion detection system for self and neighbor nodes to check for malicious neighbor. The global intrusion detection system can be deployed for clusters of mobile nodes where head node is responsible for global intrusion detection for its cluster (Dang & Mittal, 2012).

In this paper; firstly, we try to description and exploration of Intrusion detection systems such as attack categorize and models, Intrusion detection architect and technique and then we examine special IDS issues of MANETs and compare them in specified fields.

2. Attack Categorize and Models

Approximately All researchers have two categorize of attacks on the MANETs. They characterized attacks to passive and active. The passive attacks typically involve only eaves dropping of data, whereas the active attacks involve actions performed by adversaries such as replication, modification and deletion of exchanged data. In particular, Attacks in MANET can cause congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely (Sharma & Sharma, 2011; Blazevic, et al., 2001).

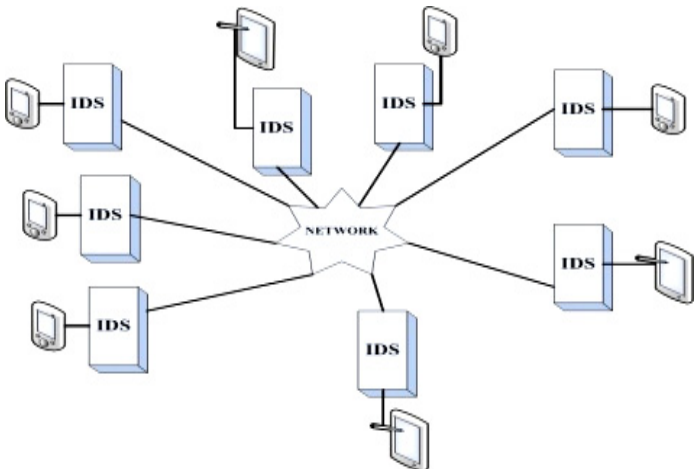

Figure1: Sample of Intrusion Detection System

In general, we can categorize MANET attacks in three categories such routing, multipart and performance (Amiri, Afshar, Naji & Ardekani, 2012). Frequency before, this topic has been discussed. In this section we only mention these names. As example of routing attacks we can aims to Routing loop attack, Blackhole attack, Link Withholding attack, Link Spoofing attack, Wormhole attack, Replay attack and Packet Modification/Insertion , multipart attacks consist of Neighbor attack, Jellyfish attack and of performance attacks we can mention DoS attacks, Sleep deprivation and Resource consumption attack.

3. Intrusion Detection Systems

Intrusion detection system (IDS) as we said before is an indispensable second line of defense since traditional prevention mechanisms are not strong enough to protect MANET (Mitrokotsa, Komninos, & Douligeris, 2008). There are three main components of IDS: data collection, detection, and response (Sen & Clark, 2008). The data collection component is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and sending data to the detection module (Sen & Clark, 2008). IDS have several highlight parts such as architecture, engine and watermarking techniques that we discuss these in this section.

3.1. IDS architecture

The existing IDS architectures for MANETs fall under three basic categories (Panos, Xenakis & Stavrakakis, 2010) (a) stand-alone, (b) cooperative, and (c) hierarchical.

- Stand-alone: in stand-alone architectures every node performs IDSs locally without collaborating and respond locally. This IDS architecture has a drawback for network attacks (Sutlu & Yilmaz, 2011).There limitation is in terms of detection accuracy and the type of attacks that they detect (Panos, Xenakis & Stavrakakis, 2010).
- Cooperative: in this architecture all nodes in MANET have their own local IDS system. Nodes come to a decision in a distributed fashion cooperatively. Upon determination of an intrusion, nodes share this information, asset attack risk degree and take necessary actions to eliminate the intrusion using active or passive precautions (Mutlu & Yilmaz, 2011).

At the same time, all the nodes participate in a global detection decision making. This is more suitable to a flat MANET (Li & Wei, 2004).

- Hierarchical: the hierarchical architectures amount to a multilayer approach, by dividing the network into clusters. Specific nodes are selected (based on specific criteria) to act as cluster-heads and undertake various responsibilities and roles in intrusion detection, which are usually different from those of the simple cluster members (Panos, Xenakis & Stavrakakis, 2010). The main advantage of this architecture is effective use of constraint resources but has a drawback for highly mobile MANETs for establishing zones and detecting responsible nodes in clusters (Mutlu & Yilmaz, 2011).

3.2. IDS engine

IDS engine is responsible for detecting local intrusions using local audit data. The local intrusion detection is performed using a classification algorithm. Firstly, it performs the appropriate transformations on the selected labeled audit data. Then, it computes the classifier using training data and finally applies the classifier to test local audit data in order to classify it as “normal” or “abnormal” (Mitrokotsa, Komninos & Douligeris, 2008).

3.3. IDS watermarking techniques

Watermarking is the method for protecting the related data that should exchange between nodes, or is imperceptible added to the cover-signal in order to convey the hidden data. Watermarking techniques are then applied in order to prevent the possible modification of the produced maps (Mitrokotsa, Komninos & Douligeris, 2007).

4. Literature Review

4.1. Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm

In this proposed algorithm (Abdelhaq et al, 2011) the researcher's aims to utilize one of the danger theory intrusion detection algorithms, namely, the dendritic cell algorithm (DCA) to detect the sleep deprivation attack over MANET. DCA is plugged in a proposed mobile dendritic cell algorithm called MDCA which represented through a proposed MDCA architecture. They tried to each node in MANET should protect itself from danger locally without using mobile agents.

The innate subsystem and the adaptive subsystem are two main component of MDCA. The proposed algorithm designed by them is as follow, at the beginning, the algorithm verifies each entered packet's ID in the memory. If that packet ID found in the detected list, this means it comes from an attacker detected before, the algorithm rejects the packet directly, deletes its information from the routing table and sends an alarm message for the second time for that packet ID. Else if the packet ID is found in the alarmed list, this means the packet comes from an attacker detected by another node so it is rejected directly, deleted from the routing table but without sending alarm again. Else, the packet must be analyzed by the packet analyzer. The packet analyzer extracts the required antigens from the routing table and generates the signals from the routing table, the availability of the bandwidth, and the power consumption rate. After that, the packet analyzer stores the antigens and signals in the antigens and signals stores respectively.

4.2. Zone-Based Intrusion Detection for Mobile Ad Hoc Networks

Bo Sun at el. in (B. Sun, K. Wu and U. W. Pooch, 2006) present a non-overlapping Zone-Based Intrusion Detection System (ZBIDS) that fits the requirement of MANETs. They present details of constructing the Markov Chain based local anomaly detection model, including feature extraction, data preprocess, detection engine construction, and parameter tuning. The whole network is divided into non- overlapping zones. There are two categories of nodes in ZBIDS, if one node has a physical connection to a node in a different zone; this node is called a gateway node. Otherwise, it is called an intra-zone node.

Only gateway nodes can generate alarms. They collect the local alerts broadcast from the intra-zone nodes and perform aggregation and correlation tasks to suppress many falsified alerts. For avoid of the single point of failure, if exist more than one gateway node in a single zone, all of which perform the alert aggregation task simultaneously.

The functionality of Local Aggregation and Correlation Engine (LACE) is to locally aggregate and correlate the detection results of detection engines. Global Aggregation and Correlation Engine (GACE) in gateway nodes is to aggregate and correlate the detection results from local nodes in order to make final decisions. They can also cooperate with neighboring gateway nodes to further exchange information. After an attack is identified, based on different attack types, the Intrusion Response Module (IRM) could take corresponding measures, such as identifying the intruders, reinitiating the communication channels, and excluding the compromised nodes from the networks.

4.3. Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms

Mitrokotsa at el. in (A. Mitrokotsa, N. Komninos and Ch. Douligeris, 2007) design and evaluate of intrusion detection models for MANETs using supervised classification algorithms. They adopt the

IDS architecture composed of multiple local IDS agents that are responsible for detecting possible intrusions locally.

They used MultiLayer Perceptron (MLP), the Linear model, the Gaussian Mixture model (GMM), the Naive Bayes model and the SVM model for classification. All these models require labeled training data for their creation.The IDS architecture they adopt is composed of multiple local IDS agents that are responsible for detecting possible intrusions locally. The collection of all the independent IDS agents forms the IDS system for the MANET. Each local IDS agent is composed of the following components:

Data Collector: is responsible for selecting local audit data and activity logs. Intrusion Detection Engine: is responsible for detecting local intrusions using local audit data. The local intrusion detection is performed using a classification algorithm. Response Engine: If an intrusion is detected by the Detection.

4.4. A game-theoretic intrusion detection model for mobile ad hoc networks

Hadi Otrok at el. in (H. Otrok at el., 2008) addresses the problem of increasing the effectiveness of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a leader node is usually elected to handle the intrusion detection service on behalf of the whole cluster. To increase the effectiveness of an IDS in MANET, they propose a unified framework that is able to: (1) Balance the resource consumption among all the nodes and thus increase the overall lifetime of a cluster by electing truthfully and efficiently the most cost-efficient node known as leader-IDS. A mechanism is designed using Vickrey, Clarke, and Groves (VCG) to achieve the desired goal. (2) Catch and punish a misbehaving leader through checkers that monitor the behavior of the leader. A cooperative game-theoretic model is proposed to analyze the interaction among checkers to reduce the false-positive rate. A multi-stage catch mechanism is also introduced to reduce the performance overhead of checkers. (3) Maximize the probability of detection for an elected leader to effectively execute the detection service. This is achieved by formulating a zero-sum non-cooperative game between the leader and intruder. We solve the game by finding the Bayesian Nash Equilibrium where the leader's optimal detection strategy is determined. Finally, empirical results are provided to support our solutions.

4.5. BeeID:Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative Selection Algorithms

In the reference (Barani & Abadi, 2012) the researchers present a dynamic hybrid approach based on the artificial bee colony (ABC) and negative selection (NS) algorithms, called BeeID, for intrusion detection in AODV-based MANETs. The approach consists of three phases: training, detection, and updating. In the training phase, a niching artificial bee colony algorithm, called NicheNABC, runs a negative selection algorithm multiple times to generate a set of mature negative detectors to cover the nonself space. In the detection phase, mature negative detectors are used to discriminate between normal and malicious network activities. In the updating phase, the set of mature negative detectors is updated by one of two methods of partial updating or total updating. We use the Monte Carlo integration to estimate the amount of the nonself space covered by negative detectors and to determine when the total updating should be done.

5. Comparison of Ids algorithms

The result of comparison shows in Table 1. We have put the number of each algorithm in the column Algorithms Name for more clarity. As Table 1 shows, algorithms just able and adequate for some of

attacks and they hadn't any pre-defined mechanism for other attacks. It appear that design and implementation a method for identify all attacks is laborious. Also the all algorithm inflict some overhead in network but this amount of overhead is difference.

Table 1. Comparison Table

Algorithms Name	Comparison fields			
	Used Method	*Types of attacks addressed*	*Over-head*	*architecture*
Detecting Sleep Deprivation Attack over MANET	Danger	sleep deprivation attack	Yes	Stand-alone
Danger Theory –Based Algorithm	Theory			
Zone-Based Intrusion Detection for Mobile Ad Hoc	Markov Chain	routing disruption attack	Yes	Cooperative
Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms	classificati on- neural network	Black Hole, Forging, Packet Dropping, and Flooding attacks	Yes	Hierarchical
A game-theoretic intrusion detection model for mobile ad	game-theoretic	Selfish attack	Yes	Hierarchical
BeeID:Intrusion Detection in AODV-based MANETs Using Artificial Bee Colony and Negative	BeeID	Flooding, Black hole, Neighbor, Rushing, and Worm hole attacks	Yes	Stand-alone

6. Conclusion

As we said before, MANETs is a collection of nodes that they are randomly placed in operational environment without any before defined structure. Firstly, nodes hadn't any information about environment, then each node is alive, they try for identify other neighbor nodes, environment and submit itself in the cluster. By attention to this said notice, MANETs are susceptible to a variety of attacks that primarily target the protocols of the transport, network, and data-link layers. We peruse in this paper IDS concept and attacks categories in first three sections, then in next section we discussed some of important algorithms in IDS and comparison them together. Almost all of designed algorithms try to detection attacks in MANET but it appears that more work must be done in the field of MANET.

References

Mitrokotsa, A., Tsagkaris M., and Douligeris, Ch. (2008) Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms, Boston: Spring, 256.

Mitrokotsa, A., Komninos, N. and Douligeris, Ch., (2007) Intrusion Detection with Neural Networks and Watermarking Techniques for MANET, Pervasive Services, IEEE International Conference.

Sun, B., Wu, K., and Pooch, U.W., (2006). Zone-Based Intrusion Detection for Mobile Ad Hoc Networks , International Journal of Ad Hoc & Sensor Wireless Networks, 3, 2.

Panos, Ch, Xenakis, Ch and Stavrakakis, I.S. (2010). A novel intrusion detection system for MANETS International Conference on Security and Cryptography.

Amiri, E., Afshar, E., Naji, H.R., and Ardekani, M. (2012). Survey on network access control technology in MANETs , Malacca: IEEE 2012.

Lundin, E., Jonsson, E. (2002). Survey of intrusion detection research. Technical report 02-04, Dept. of Computer Engineering, Chalmers University of Technology.

Barani, F., & Abadi, M.I., (2012). BeeID: intrusion detection inAODV-based MANETs using artificial bee colony and negative selection algorithms, The ISC International Journal of Information Security, 1, 4.

Otrok, H., et al. (2008). A game-theoretic intrusion detection model for mobile ad hoc networks, Elsevier Computer Communications, 31.

Blazevic, L., et al. (2001). Self-organization in mobile ad-hoc networks: the approach of terminodes, IEEE Communications Magazine.

Abdelhaq, M., et al (2011). Detecting sleep deprivation attack over MANET using a danger theory – based algorithm, International Journal on New Computer Architectures and Their Applications, 3, 1.

Dang, N., & Mittal, P., (2012). Cluster based intrusion detection system for MANETS, International Journal of Computer Applications & Information Technology, 1, 1.

Sharman, R., & Sharma, S., (2011)., Performance analysis of intrusion detection in MANET, Computer Technoligy and Applications. 3, 2

Mutlu, S., & Yilmaz, G., (2011). Distributed cooperative trust based intrusion detection framework for MANETs, The Seventh International Conference on Networking and Services.

Sen, S., & Clark, J.A. (2008). Intrusion Detection in Mobile Ad Hoc Networks, Guide to Wireless Ad Hoc Networks, Springer.

Li, Y., & Wei, J. (2004). Guidelines on selecting intrusion detection methods in MANET, Proceedings of the Information Systems Education Conference, 21.